CYBERCRIME

Criminal Threats from Cyberspace

SUSAN W. BRENNER

Greenwood
PUBLISHING GROUP

Cybercrime

Recent Titles in
Crime, Media, and Popular Culture

Media Representations of September 11
Steven Chermak, Frankie Y. Bailey, and Michelle Brown, editors

Black Demons: The Media's Depiction of the African American Male Criminal Stereotype
Dennis Rome

Famous American Crimes and Trials, Volumes 1–5
Frankie Y. Bailey and Steven Chermak, editors

Killer Priest: The Crimes, Trial, and Execution of Father Hans Schmidt
Mark Gado

Cybercrime

Criminal Threats from Cyberspace

Susan W. Brenner

Crime, Media, and Popular Culture
Frankie Y. Bailey and Steven Chermak, Series Editors

PRAEGER
AN IMPRINT OF ABC-CLIO, LLC
Santa Barbara, California • Denver, Colorado • Oxford, England

Library of Congress Cataloging-in-Publication Data

Brenner, Susan W., 1947–
Cybercrime : criminal threats from cyberspace / Susan W. Brenner.
p. cm. — (Crime, media, and popular culture)
Includes bibliographical references and index.
ISBN 978–0–313–36546–1 (hard copy : alk. paper) — ISBN 978–0–313–36547–8 (ebook)
1. Computer crimes. 2. Computer networks—Law and legislation. I. Title.
HV6773.B75 2010
364.16´8—dc22 2009048693

ISBN: 978–0–313–36546–1
EISBN: 978–0–313–36547–8

14 13 12 11 10 1 2 3 4 5

This book is also available on the World Wide Web as an eBook.
Visit www.abc-clio.com for details.

Praeger
An Imprint of ABC-CLIO, LLC

ABC-CLIO, LLC
130 Cremona Drive, P.O. Box 1911
Santa Barbara, California 93116-1911

This book is printed on acid-free paper ∞

Manufactured in the United States of America

Contents

Series Foreword

This book is an outstanding contribution to the interdisciplinary series on *Crime, Media, and Popular Culture* from Praeger Publishers. Because of the pervasiveness of media in our lives and the salience of crime and criminal justice issues, we feel it is especially important to provide a home for scholars who are engaged in innovative and thoughtful research on important crime and mass media issues. It seemed essential to include a book in the series that examined the dynamic nature of cybercrime.

Many of us have a limited knowledge of the crimes that occur in the world of computers and the Internet, known as "cybercrimes" because they occur in "cyberspace." These crimes run the gambit from scams and fraud to stalking and even terrorism. These crimes have the potential for extraordinary impact on the lives of individuals and on society as a whole. Although many people fear street crimes involving face-to-face interactions with violent strangers, they are unaware of the predatory possibilities of an e-mail solicitation.

Cybercrime is not an altogether new breed of crime. As Professor Brenner explains in this book, the crimes carried out by this new breed of criminal often reflect emotions as old as humankind. These emotions include greed, obsession, or a desire for revenge. What is new is the space in which the crimes are played out. The cybercriminal and his or her victim may be only miles apart or a world away from each other. Scam artists on another continent can seduce those inclined to avarice into parting with their money. An

obsessed acquaintance can go into cyberspace and stalk the object of his or her desire. Another can seek revenge by assuming the identity of the victim to post photos on a porn site or leave angry or embarrassing messages about the victim on a another site. And it can all be done while the cybercriminal sits at his or her computer.

Cybercrime raises issues of privacy, or rather, the increasing loss of privacy. The use of the computer for legitimate activities—from banking and social networking to searches for employment—is a commonplace, almost taken-for-granted aspect of modern life. However, the information that we send into cyberspace makes us vulnerable to cybercrime. The details of our identities and our activities, once shared online, become accessible to those who would steal and misuse the information.

From the beginning, as Professor Brenner discusses, cyberspace attracted "hackers," a breed of outlaw computer whizzes who attacked sites, such as federal agencies, to prove that it could be done. These young outlaws sometimes were recruited to develop ways of protecting the sites they had penetrated. In recent years, for professional criminals who hack into sites, it has been done for the money that can be made from crimes such as corporate extortion. The lack of a sufficient number of law enforcement and security experts trained in detecting and eradicating cybercrime means that organizations and agencies remain at risk from cyberattacks.

The goal for agencies such as the Federal Bureau of Investigation (FBI) is to reduce, if not eliminate, this risk by capturing the criminals. However, the techniques that have been developed to prevent computer intrusions frequently lag behind the ability of cybercriminals to develop a new virus or to carry on their activities beyond the reach of the U.S. government. The increased risk post-9/11 of a terrorist attack launched in cyberspace is no longer the stuff of science fiction.

At the same time, there are some issues, such as invasion of privacy of suspects or the censorship of free speech concerns, with which we must deal. At what point would such concerns be suspended in pursuit of the cybercriminal?

In this book, Professor Brenner provides an accessible and informative exploration of the history of cybercrime, the various categories of cybercrime, and the law enforcement response. Drawing on true cases of cybercrime and fictional depictions in popular culture, Professor Brenner tells us what we need to know about the new world created by the expansion of computer technology. As she illustrates, although there are reasons for concern about

cyberspace, we can only go forward into this brave new world. As the technology evolves, the responses of both citizens and the criminal justice system must also evolve.

Frankie Y. Bailey and Steven Chermak,
Series Editors

This page intentionally left blank

1

Twenty-First Century *Twilight Zone*: Stalking a Town

INTRODUCTION

In the *Twilight Zone* episode "The Monsters Are Due on Maple Street," aliens from another planet manipulate the residents of a sleepy Midwestern suburb into turning on each other in what becomes an orgy of violence.[1] The aliens do this by turning the suburbanites' technology against them on a summer evening. They begin by shutting off phone and electric service to the suburb.

As the residents gather in the street to speculate about what is happening, one of them named Pete leaves, saying he will walk to the next suburb and find out what "is going on." Those left behind speculate about the outages and the odd things that preceded them: a flash of light, something passing overhead, and a loud roar. A man named Les tries unsuccessfully to start his car. As he walks away from the vehicle, the aliens start it remotely, with no one inside. This causes the other, already unnerved residents to think Les must be "in on" whatever is happening to them. They begin to interrogate Les about why he spends nights in his backyard, looking up at the sky. A boy who reads science fiction says the mysterious events are part of an invasion by "space aliens," some of whom would have infiltrated the suburb disguised as humans. By now, night has fallen, and the residents still have no electricity, no transportation, and no communication.

Les says he is an insomniac and goes to the backyard when he cannot sleep. As he tries to explain his behavior, the lights go on in his home and loud music blares from inside. The others become even more suspicious. A neighbor named Steve tries to defend Les, which makes the crowd also suspect him of being involved in whatever is happening to them. Charlie, a loud and aggressive resident, begins cross-examining Steve about a mysterious radio he claims to be building but no one has seen. At that point, the terrified crowd sees a silhouetted figure—maybe a "space monster"—walking toward them. Frightened, like the others, Charlie grabs a shotgun and shoots at the figure, killing Pete, who had walked to the next suburb to find out what was going on.

As Charlie claims it was self-defense, the lights come on in his house, and the crowd turns on him. He runs for home, with the others chasing him and throwing stones. After being hit by a stone, he stops and tries to deflect the crowd by blaming the boy who told them an invasion was coming. ("How did he know?")As the crowd turns on the boy, lights and telephones start going on and off in other houses, and cars and lawn mowers begin to start and stop for no apparent reason. The residents of Maple Street descend into madness, smashing windows and attacking each other.

The scene shifts to a hillside overlooking the suburb. Two aliens stand by their spaceship, watching the riot on Maple Street. One of them notes how easy it is to turn humans against each other by tinkering with the technology on which they rely.

When this *Twilight Zone* episode aired in 1960, the only entities that could have implemented the scenario it depicts were the utility companies . . . and, perhaps, space aliens. That is no longer true. As we will see in this chapter and in succeeding chapters, our ability to use cyberspace alters the fabric of our lives in fundamental and irreversible ways. The most significant aspect of cyberspace for our purposes is that our access to it erodes the monopolization of power by governments and corporations.

In 1960, only the electric company would have been able to turn the power on and off on Maple Street, and only the telephone company could have done the same with the phone service. Back then, utility companies (and government agencies, banks, and other private entities) were the masters of their respective domains. Someone bent on harassing the residents of Maple Street could have shut off the phone or electric service by cutting cables but would not have been able to tinker with the services, turning them on and off selectively. In 1960, the world revolved around tangible assets and resources; utility companies and other public and private entities could secure their assets and their processes behind walls, fences, and doors. They

could screen and limit those who had access to the premises and the assets they protected. They could, in sum, keep the rest of us, including "the bad guys," out.

Almost 50 years later, that has changed. Walls, fences, and doors still keep people from physically invading protected places, but physical access is no longer the only option. Today, people with sophisticated computer expertise—commonly known as "hackers"—could replicate the tactics the aliens used on Maple Street except, perhaps, for remotely turning cars and lawn mowers on and off. As we will see in later chapters, cyberspace makes what used to be physically secured areas accessible to anyone with the requisite, often minimal, level of computer expertise. As a result, we effectively live in a world with four dimensions (five if you include time): the height, length, and width of real space plus virtual space. Virtual space lets those of us who are law-abiding citizens do marvelous things. Unfortunately, as we shall see, it also lets those of us who are less law-abiding break rules and wreak havoc in various ways.

Perhaps no case better illustrates the power cyberspace gives us to wreak havoc in new and terrifying ways than a 1999 incident in which a man effectively replicated the aliens' manipulation of the hapless residents of Maple Street.

STALKING A TOWN

Townsend is a small town in northern Massachusetts, located about 55 miles from Boston. Townsend was incorporated in 1732 and had 9,501 citizens by 2000. It has four schools: a high school, a middle school, an elementary school, and a preschool. The middle school—Hawthorne Brooke—has approximately 600 students in grades six through eight and 60 faculty and staff members.

In the fall of 1999, some Hawthorne Brooke eighth-graders were spending time after school in an online chat room for Limp Bizkit fans.[2] They used the room to talk about personal things, as well as the band. At one point, a new personwho said he was a Hawthorne Brooke student began hanging out in the chat room. Because he was from Hawthorne Brooke, the others invited him to join them in their private chat room. He did and soon was always there, ready to talk to the others and hear about how their days had gone, what was happening at home, whom they liked, and whom they didn't . . . all the things children of that age talk about.

The new person began to say and do strange things. He said he was a serial rapist and would be coming for them. And he sent them to child

pornography that was posted online, which included horrific images of a five-year-old girl being raped. When the others pressed him to tell them who he was, he said he was an eighth-grader they talked about in the chat room. The others retaliated by harassing the innocent boy at school.

By October, the students were beginning to wonder if he really was a Hawthorne Brooke eighth-grader, both because of his increasing erratic behavior and because he was making mistakes when he talked about the school. Some of them finally told him they didn't believe he was a student at their school, which seemed to infuriate him. He said he was going to blow up their school because they didn't believe him.

On October 19, he sent them a link to a Web site with photos posted on it. One was an image of Hawthorne Brooke Middle School with the cross hairs of a rifle scope superimposed on it. Another was a photograph of the school principal, altered to make it look as if he was bleeding from bullet holes in his head and chest. The site also lauded the high-school students who had carried out the Columbine school shootings five months earlier. On October 20, the mystery person added a "hit list" to the site. It listed the first names of 24 Hawthorne Brooke students and the last names of three teachers. Under the list was this sentence: "You lucky individuals will go home with more holes in your body than you came with."

The students were terrified. When they told their parents what was going on and showed them the site, the parents were terrified, too. No one knew what to do, and no one knew whom to trust. It was clear that the mysterious person in the chat room was a local because he knew so much about what had gone on in the school from day to day—who wore what, who sat with whom at lunch, who was mad at whom, and so on.

Police and school officials held a meeting with the parents of the students whose names were on the "hit list," but no one really knew what to do about the person who posted it. Panic set in as the community realized they were at the apparent mercy of an unknown psychopath. As a member of the community noted later, their tormentor made it seem that violence was imminent, and in a post-Columbine world, everyone—students, teachers, and parents—was terrified and suspicious of each other. Everyone knew the person responsible *had* to be someone affiliated with the school; otherwise, how could he know so much about it? So students suspected their teachers, the staff at the school, and each other; parents suspected teachers, staff members, and every child but their own; and teachers and staff members suspected each other and their students. The climate must have been unimaginable.

The morning after the meeting, police used bomb-sniffing dogs to search the halls and classrooms at Hawthorne Brooke. They found nothing. They

assigned an officer to the school, to be on the lookout for . . . whatever. As students arrived, teachers searched their book bags, looking for weapons or anything suspicious—anything that might identify the person who was responsible for all of this. Many parents simply refused to send their children to school, and some teachers quit.

At that point, their mysterious tormentor took things offline and into the real world. The mother of a girl who was on the "hit list" was a secretary at Hawthorne Brooke. When she answered a call to the school, all she heard was music. Police later identified it as a song linked to the Columbine shootings. When the woman got home, the same music had been left on the family's answering machine. Her husband was so upset he went to his brother to borrow a gun to protect his family from the person who was terrorizing their town. His brother talked him out of it.

When it seemed as if disaster would strike at any minute, the police got a break. Working with the state police, Townsend officers traced the mysterious person's Internet activity to the Maple Woods Community College in Missouri. They later traced the calls to the school and the family's answering machine to a pay phone at the same college. At that point, the police assumed the perpetrator was in Townsend and was working with someone in Missouri to make it seem that the online activity and calls were coming from there.

As the Massachusetts officers worked with their Missouri counterparts, it began to become apparent that their perpetrator was not, and had never been, in Townsend. The mysterious figure who terrorized a town and turned neighbor against neighbor was a 19-year-old paraplegic from Smithville, Missouri: Christian Hunold.[3]

Hunold's mother was the chief financial officer for a local school district; his father was a retired high-school teacher. Until he was 15 years old, Hunold was an honor-roll student who played soccer and participated in his school band. When he was 15, he took a ride with a friend who had just gotten his driver's license. They were on their way to a mall when the driver lost control of the car, and it smashed into a tree. Hunold was badly injured. He eventually regained the use of his arms and some use of his hands, but he would never walk again.

As the years passed and Hunold graduated from high school, his parents and friends all thought he had put the accident behind him, but he had not. He resented being physically dependent on his parents; and he seethed about the unfairness of having lost everything—sports, music, the ability to lead a regular life—while the person who was responsible for the accident, the driver, walked away essentially unharmed.

Isolated at home in his wheelchair, Hunold discovered he was good at computer programming and Web design, and he decided to study computer science at a community college. As he spent hours on the family computer, he discovered something else: He could be a different person—a strong, whole person—in cyberspace. By the time he found his way into the Limp Bizkit chat room and met the Hawthorne Brooke students, he was spending eight hours a day online, escaping the life he hated.

As Hunold got to know the Hawthorne Brooke students, he found he hated their childish obsessions and complaints, and he decided to give them a taste of "the real world." He later told investigators he was able to pass as a Hawthorne Brooke student for so long because he spent a lot of time listening to the students talk to each other and talking to them individually. When he chatted with students, Hunold would ask about their families, their houses, their pets, and who they hung out with at lunch and other times. Thus, he acquired the information he used to convince them he was one of their classmates. As Hunold grew adept, he could chat knowledgeably about who lived where or wore what or had a dog (and what the dog's name was) He could even chat about who sat with whom at lunch and what someone wore to school that day. One thing that made his pretense so successful was that he dealt with children, who tend to be more gullible than adults.

Hunold said he began threatening the Hawthorne Brooke students when he began to lose control of the charade—when they began to doubt that he was a student at their school. When interviewed at his home in Missouri by two Massachusetts officers, Hunold seems to have vacillated between expressing remorse and dismissing the affair as a joke. He told the officers he never had any intention of going to Townsend to carry out the threats he made and probably would not have been physically able to do so, in any event.

Perhaps the most chilling thing that came out of the officers' visit to the Hunold home was a discovery they made when they searched the computer he used to terrorize the people of Townsend. On it, they found evidence they believed indicated that he was preparing to stalk another school—in Georgia, this time. If he not been caught when he was, Hunold might have gone on to stalk the Georgia school and other schools in other states. If he had continued, he probably would have been much better, more believable, and more terrifying the second time and with each succeeding iteration.[4]

If Hunold had been more sophisticated in his use of cyberspace, his career as a stalker of schools might not have been interrupted, at least not until after he terrorized more communities. If he had hidden his tracks—if he had made it appear he was using a computer in Massachusetts or Ohio or California—he probably would not have been caught, especially in 1999.

Cybercrime was a very new phenomenon then, and few law enforcement agencies were adept at investigating it. The Massachusetts investigators were able to track Hunold because the state had a computer crimes unit and because he apparently made no effort to hide his tracks, either when he was online or when he called the school.

The Hunold case is old news now. Cybercriminals have moved far beyond the relatively simple tactics he used to carry out his crime. But what Hunold did still perfectly exemplifies the distinctive aspects of cybercrime: A crippled boy was able to manipulate and terrorize people in a town 1,000 miles away. His use of virtual space gave him abilities no one has in the real world, where we are subject to the laws of gravity and the rules of physics. In the next four chapters, we will see how these virtual-space abilities create new crimes and alter traditional crimes. In Chapters 8 through 10, we will see how they create major challenges for law enforcement officers and, in so doing, erode the likelihood that clever cybercriminals will be caught and punished.

This page intentionally left blank

2

From Mainframes to Metaverse: The Origins and Evolution of Cybercrime

In this chapter, we trace the evolution of modern cybercrime as a new type of criminal activity. We will touch on the legal issues cybercrime raises but will examine them in detail in Chapters 3 through 5.

WHAT IS CYBERCRIME?

Before we can trace the evolution of cybercrime, we need to define what it is. More precisely, we need to distinguish "cybercrime" from "crime."[1]

"Crime" consists of engaging in conduct that has been outlawed by a society because it threatens the society's ability to maintain order. Order cannot exist without rules that proscribe certain "harmful" activities and institutions that enforce these rules. These rules constitute a society's criminal law. Criminal law is designed to prevent the members of a society from preying on each other in ways that undermine order. It does this by defining certain types of behavior as intolerable as "crimes."

Crimes take many forms because each targets a specific "harm." Crimes target harming individuals (murder, rape), property (arson, theft), government (obstructing justice, treason), and morality (obscenity, gambling).

Because societies have dealt with crime for millennia, they have developed standardized definitions of real-world crimes.

"Cybercrime" also consists of engaging in conduct that is outlawed because it threatens order. Cybercrime differs from crime primarily in the way it is committed: Criminals use guns, whereas cybercriminals use computer technology. Most of the cybercrime we see today simply represents the migration of real-world crime into cyberspace. Cyberspace becomes the tool criminals use to commit old crimes in new ways.

THE EMERGENCE OF CYBERCRIME (1950–1990)

This section traces cybercrime from its origins in the era of mainframe computers to 1990, when the Internet and personal computers were becoming more sophisticated and more pervasive. The next section outlines its evolution from 1990 to the present.

Mainframes and the Rise of Hacking

The first published reports of computers being used to commit crimes appeared in the 1960s, when computers were large mainframe systems.[2] The history of modern computing dates back to the nineteenth century, but the development of the mainframe business computer did not begin until after World War II.[3] In 1946, several companies began working on a commercial mainframe, and by 1951, the UNIVAC (UNIVersal Automatic Computer), created by the company of the same name, was being used by the Census Bureau.[4] In 1951, CBS used a UNIVAC to predict the outcome of the presidential election, which helped to popularize the new technology.[5] By 1960, 5,000 mainframes were in use in the United States; by 1970, almost 80,000 were in use in the United States and another 50,000 were in use abroad.[6] Given the tremendous increase in the number of computers, it is not surprising that computer crime began to become an issue in the 1960s.[7]

Computer crime in the 1960s and 1970s differed from the cybercrime we deal with today. There was no Internet; mainframes were not networked to other computers. In 1960, a typical IBM mainframe cost several million dollars, needed an entire room to house it, and needed a special air-conditioning system to ensure that its vacuum tubes would not overheat and fry the data in the computer.[8] A mainframe needed a group of specialist technicians to ensure that "its innards wouldn't melt" if the air conditioning went off and to generally keep it up and running.[9] Only a select group of researchers were

allowed to use a mainframe. To access a mainframe, a researcher gave the data he or she wanted the computer to analyze to a keypunch operator, who used a machine to punch holes in manila cards.[10] The holes encoded the researcher's data into a form the machine could read. The cards were then given to another operator, who fed the cards into a machine that transmitted the information to the mainframe. At some point, the researcher would receive a printout showing the machine's analysis of his or her data.

Because mainframes were not networked with other computers, and because the only way to access a mainframe was by using this cumbersome process, only a few people were in a position to commit computer crime. They were the "insiders"—people whose employment gave them access to a mainframe computer.[11] That influenced the kind of computer crimes that were committed in this era. Insiders sometimes spied on other employees by reading their confidential files; and they might sabotage a computer or the data it contained as retaliation for being fired or disciplined.[12] These crimes occurred, but the most common type of computer crime in this era was financial; insiders used their access to a mainframe computer to enrich themselves.

In the mid-1960s, for example, "Val Smith" (an alias) was an accountant for a company in his hometown.[13] He also used a "small UNIVAC" he owned to provide the company with computing services. Over time, Smith became convinced the company was abusing him and cheating him out of money he had earned. Smith decided to use his control over the company's accounts and computing system to recoup "his share of the profits." He set up dummy companies to provide imaginary services to his employer and billed the company for their nonexistent efforts. Smith used the computer to automate the billing process; he also used it reduce the amount of the company's reported profits and took "his" money from the unreported excess. He was so successful that within a year or so, he was making $250,000 a year, an astonishing income for a 1960s-era accountant in a small town. Smith later said it was easy to conceal the embezzlement from his bosses because they believed any figures that came from a computer were infallible.

After six years, Smith had accumulated a million dollars and decided to quit. He did so by making a deliberate error that was discovered and led to his being charged with several crimes. Smith pled guilty because he believed he would only get 18 months in jail, and he thought 18 months was a fair exchange for the million dollars he still had. Unfortunately for him, the judge sentenced Smith to serve 10 years; while in prison, he earned a college degree and taught courses to other prisoners, all of which resulted in his being

paroled after 5-1/2 years. He came out of prison a free man with a million, tax-free dollars at his disposal and never had to work again.[14]

The outcome of Smith's story—getting away with a million dollars—is unique, but his crimes were not. Many computer embezzlement cases came to light during this era, even though companies often did not report the crimes to the police.[15] In a California case, a teller used his access to the bank's computer to embezzle more than $100,000 from his employer. Instead of turning him in to the police, his employer promoted him to a higher-paying position, on the condition he never explain what he did to other tellers.[16] As Senator Abraham Ribicoff noted, banks that would call the police if a gunman robbed them would "say nothing" to police when an insider used a computer to steal: "They would rather absorb the loss than call in the police. They are fearful of bad publicity."[17] As we will see, businesses are still reluctant to report cybercrime for fear of bad publicity.

Bank employees were not the only insiders committing computer crimes in the 1960s. In 1964, executives of Equity Funding Corporation of America, an insurance company, began a 10-year scheme in which they used the company's computers to inflate its earnings.[18] At the beginning, they simply entered false commission income—eventually totaling $85 million—into the computerized accounting system. Because blatant false entries were relatively risky, they later moved to a different approach: showing that the company had sold more policies than it actually had. When the scheme collapsed in 1973, the Equity computers showed that the company had sold 97,000 insurance policies; it had actually sold fewer than 33,000. Federal investigators said two-thirds, or $2 billion dollars' worth, of the insurance the company claimed to have written was fraudulent.[19] After the fraud was discovered, Equity went bankrupt—in what was then the second largest bankruptcy ever—and 22 of its officers and employees were convicted of federal criminal charges.[20]

While embezzlement and fraud were the most common crimes, employees found other ways to profit from their access to a mainframe. Some stole information and sold it; they usually took trade secrets, but in one case, employees of the Drug Administration Association stole the names of informants and information about pending investigations and sold it to drug dealers.[21] Other employees had the company computer issue phony payroll checks to nonexistent employees, which they, of course, cashed.[22] Another less common tactic was to misappropriate company data and hold it for ransom.[23]

The crimes committed in this era all had one thing in common: The victims were a company or a government agency because large entities were

the only ones who used mainframe computers. Furthermore, mainframes were generally incapable of inflicting "harm" on an individual. It might have been possible for an insider to manipulate mainframe data to fire someone improperly, but that would have been a very risky crime. The victim would probably complain, triggering an inquiry that could lead to the unraveling of this scheme and any others in which the perpetrator was involved. Using computers to "harm" individuals did not become a problem until the 1980s, when the "personal computer" appeared.

Because only insiders could commit mainframe crime, it consisted of committing old crimes a new way. And because mainframe crime was purely internal, it did not empower criminals the way cyberspace empowered Christian Hunold. That was the product of developments we examine in the next sections.

Phone Phreaking

The term "phone phreaking" is based on a *portmanteau*—a word created by blending other words.[24] "Phone" and "freak" were blended to create "phreaking" and "phreak" (as in "phone phreak"). Phone phreaking consists of using various devices to experiment with and manipulate a phone system.

The origins of phone phreaking are murky. Most accounts trace its beginnings to 1957, when an eight-year-old blind boy named Joe Engressia learned that whistling a particular tone (the E above middle C) into a telephone gave him access to the system.[25] Engressia was the first civilian to discover the 2600-Hz frequency, which the telephone company used to take control of its trunk lines; with control of a trunk line, he could make free calls to anyone, anywhere in the world. As he grew older, Engressia learned more about how to manipulate the phone system and shared his knowledge with others.[26]

Because Engressia had perfect pitch, he could create a 2600 tone by whistling. Others could not. They had to come up with devices to create the tone. At first, they used electronic organs or synthesizers, recording the tone and playing it back to activate a trunk line. In the late 1960s, someone realized that the toy whistle included as a prize in boxes of Cap'n Crunch cereal produced a perfect 2600 tone. As a sort of homage, John Draper, who became a legendary phone phreak, began using the alias "Captain Crunch" (his spelling) to hide his identity.[27] By 1970, the whistle had been superseded by devices—"blue boxes"—that generated the 2600 tone.[28]

Phone phreaks did not consider their activity to be illegal, even though they were stealing services from the telephone company; theft of services is

a crime in most, if not all, states.[29] Phreaks thought of themselves as researchers, not criminals. In a 1971 *Esquire* interview, Joe Engressia said he phreaked for "the pleasure of pure knowledge. There's something beautiful about the system when you know it intimately."[30]

Unfortunately for the phreaks, the *Esquire* article brought law enforcement down on them: Soon after the article appeared, police broke into Engressia's apartment in Memphis and arrested him for theft of services.[31] The charges were reduced and the jail sentence he received upon being convicted was suspended . . . on the condition that he never phreak again.[32] Engressia, who had an I.Q of 172, did menial work for the phone company until 1988, when he chose to be five years old for the rest of his life. He died in 2007, having spent his last years living on disability payments in an apartment full of toys and stuffed animals.[33] The blind security analyst—"Whistler"—in the 1992 hacker movie *Sneakers* was apparently based on Engressia.[34]

The *Esquire* article also caused trouble for other phreaks, including Captain Crunch. He was arrested on federal wire fraud charges, convicted, and sentenced to five years of probation. It was the first of three arrests, convictions, and sentenced he would receive. He seemed unable to resist phreaking until he discovered computers in the early 1980s. Draper spent years working as a software programmer and computer security consultant, but his career fell into decline with the beginning of the twenty-first century.[35] Like Draper, other phone phreaks became interested in the technology, and many became hackers, as we will see in the next section. Traditional phone phreaking was dead by the 1990s, a casualty of the shift to digital call switching.[36]

Hacking

The term "hacker," and much of what would become hacker culture, emerged from the Massachusetts Institute of Technology's Artificial Intelligence Laboratory in the late 1950s.[37] Some MIT students were interested in computers and programming, but they had a problem: The only computers were mainframes, and only faculty and other "important" users were authorized to use the MIT mainframes. A sympathetic computer technician eventually let the students use a special mainframe on loan to MIT, where they could interact with this computer instead of having to use the punch card-reader process. By working with the computer, the students learned how to program it to make it "do" things. In other words, they learned to "hack," but "hacking" did not have the destructive, illegal connotation it

has today. At MIT, a "hacker" was "someone who does . . . interesting and creative work at a high intensity level."[38]

An MIT "hack" was a clever practical joke, similar to elevator hacking: The buttons on an elevator were rewired, so that pushing the button for the second floor sent the person to the twentieth floor.[39] The "Cookie Monster" was a popular MIT computer hack in the 1970s: As someone worked at a computer terminal, the machine would begin to flash "Give me a cookie" and similar messages, making the person think their work had been lost.[40] The program would eventually flash "I didn't want a cookie anyway" and disappear, leaving the work unharmed. If the victim typed "cookie" when the attack began, the screen would display "thank you," and the attack would end.[41]

A culture of hacking grew up at MIT and spread to other centers of academic computing. It was based on an informal ethos, which held that access to computers "should be unlimited and total."[42] Hackers freely explored computer systems; they shared what they learned and created. When a hacker created a program, he (they were almost always male at this time) would distribute it to others, to be used and improved. Of course, this ethos evolved at a time when computers were closed systems and software had not become a commercial product.[43]

That began to change in 1969 when the ARPANET—Advanced Research Projects Agency Network, the first packet-switching network—went online.[44] It linked mainframes in hundreds of universities, research laboratories, and defense contracting companies. It also linked hackers, transforming them into "a networked tribe."[45] This second-stage hacker culture evolved over the next decade. Because ARPANET could link a maximum of 256 computers,[46] hacker culture was limited to a relatively small group until the 1980s, when the personal computer brought it to a much wider audience.

The popularization of hacking was the result of two innovations: the Internet and the personal computer. Three personal computers—the Apple II, the PET 2001, and the TRS-80—hit the market in 1979; "over half a million . . . were sold," and computing ceased to be a niche activity reserved for specialists.[47] The era of the *War Games* hacker had begun.

As the *New York Times* noted in 1983, the number of "young people roaming without authorization through" the country's computer systems was in the thousands and growing "hand-in-hand with the boom in personal computers."[48] The *Times* article was one of many stories about hackers that appeared in 1983, most prompted by the FBI arresting a group of Milwaukee hackers known as the 414s (after the local area code).[49]

The 414s were six boys between the ages of 16 and 22 who met in an Explorer Scouts group. Using personal computers and dial-up modems, they hacked into more than 60 computer systems, including the Memorial Sloan-Kettering Cancer Center, Los Alamos National Laboratory, and Security Pacific Bank in Los Angeles. They destroyed data in at least two of the systems they hacked. The 414s were caught because they came back to the same computers over and over. A system administrator figured out what was happening and called the FBI. The FBI used wiretaps to track the 414s to their homes in Milwaukee. Only two were prosecuted (for making harassing phone calls); the other four agreed to stop hacking and pay restitution for the damage they had caused. The two who were prosecuted pled guilty and were sentenced to probation.

When he testified before Congress, one of the 414 hackers said the group was inspired by the movie *War Games*. In 1984, four teenagers suspected of hacking into the NASA Marshall Space Flight Center reportedly told police they used techniques they learned from the same film.[50] These were not the only instances in which life imitated art. Markus Hess, a German hacker recruited by the KGB to spy on U.S. military systems, was inspired by *War Games*. He vowed that he, similar to the movie's protagonist David Lightman, would hack NORAD, the North American Aerospace Defense Command in Colorado.[51] Hess was not able to hack NORAD, but he hacked 400 U.S. military computers, including a Pentagon database.[52]

In addition to accurately depicting how a hacker accessed a remote system, *War Games* romanticized hackers.[53] As *Wired* noted 25 years later, it was the "geek-geist classic that legitimized hacker culture" and "minted the nerd hero."[54] *War Games* brought the concepts of "hacking" and "hackers" to the attention of American society. It initially popularized the image of hackers as creative but benign, but that image rather quickly began to change. The arrests of the 414s and others engaged in similar activity indicated hackers were anything but benign. The image of hackers was further tarnished by a wave of publicity about FBI efforts to deal with hackers' online depredations.[55] In 1984, a hacker-turned-FBI informant estimated hackers stole $100 million a year in long-distance service, pirated the same amount of software, and were responsible for $200 million a year in credit card fraud.[56] In the mid-1980s, news stories reported that hacking had become "an epidemic" among high-school students.[57]

The essentially innocent image of *War Games*' David Lightman hacking a system to find a new game morphed into the image of a hacker as a criminal. Both images survive. "Hacker" has come to have two distinct meanings: hacker as a brilliant programmer, and hacker as a computer criminal. To

differentiate the two, hacker jargon divides hackers into two categories. "Black hat" hackers use their computer skills to commit crimes, whereas "white hat" hackers use theirs for "altruistic or at least non-malicious reasons."[58] As is probably obvious, the categories "derive from the dress code of formulaic Westerns, in which bad guys wore black hats and good guys white ones."[59]

In the post-*War Games* 1980s, a number of hacker groups arose to exploit the opportunities available in what was now known as "cyberspace," a term introduced in William Gibson's novel *Neuromancer*.[60] A juvenile known as Lex Luthor created the Legion of Doom (LOD) in 1984.[61] Some LOD members were white hats driven by intellectual curiosity; others were blackhats pursuing "for-profit computer crime."[62] In 1989, LOD member Phiber Optik was expelled for reasons that are still unclear.[63] What is clear is that Phiber Optik (a high-school student, like most of the others), Acid Phreak, Scorpion, Corrupt, and Outlaw decided LOD had "outlived its reputation" and created a new group: the Masters of Deception (MOD). As one source notes, the name "perfectly suited" the group, which used "artful deception" of various types to attain "new heights" in understanding computer systems.[64]

The MOD and the LOD became infamous when they fought the Great Hacker War in 1990–1991. The first flare-up came when LOD accused a MOD member of using information from a LOD bulletin board to start a security company. The war began when MOD members joining a conference call intended to settle things heard LOD members using racial epithets to describe members of MOD.[65] At first, they played phone pranks (e.g., shutting off service, arranging for phones to ring continuously) on each other. Things escalated when a LOD member used a computer program to translate "The History of MOD" into racist jive. As things escalated, MOD members began to cross the line into serious criminal activity. They hacked phone systems to obtain free services; they also hacked information services such as TRW to obtain personal information that they sold or used to harass their rivals and others. In 1991, five members of MOD were indicted on federal criminal charges, including conspiracy, wire fraud, computer fraud, computer tampering, and wiretapping.[66] All of them pled guilty, and all were given some time in jail.[67] No LOD members were charged; the LOD seems to have dissolved after apparently losing the war.

As the 1980s turned into the 1990s, hacking was changing. Personal computers and software—including the software being developed specifically to facilitate hacking—were much more common. So were targets. In the 1970s and most of the 1980s, it was a challenge "just to find a system to

hack"; by the 1990s, the Internet was starting to link everything, which meant hackers had thousands, and eventually millions, of targets.[68] Because most organizations did not realize the need to secure their computers, most targets were wide-open, easy pickings for hackers. But hackers had to deal with a new phenomenon: law enforcement, which was becoming aggressive in pursing notorious hackers, such as Los Angeles' "Dark Dante."

Kevin Poulsen—also known as Dark Dante—began phreaking when he was in his early teens,[69] and moved on to hacking after his parents bought him a TRS-80 computer and modem for this sixteenth birthday.[70] In 1982, Poulsen left high school after the eleventh grade and became Dark Dante. He and another hacker broke into computer systems, preferably ones owned by the U.S. Department of Defense. In August 1983, they hacked several think tanks that worked on classified military projecs. In September, police arrested Poulsen's hacker comrade, who was 19 and could be tried as an adult; he was convicted of "malicious access" to computers and spent less than two months in jail.[71]

Because Poulsen was 17, he could not be tried as an adult; no charges were ever brought against him for this episode. Instead, Poulsen was hired by one of his victims. SRI International, which conducted classified research for the military, hired him to teach the military how to safeguard its computers.[72] Poulsen had a security clearance, a more than adequate salary, and a condo near his job in northern California; he worked on a variety of projects, including the Strategic Air Command's computer systems.

Things begin to fall apart in February 1988, when the owner of a storage rental facility entered a unit because its rent had not been paid.[73] He found what he thought was stolen property and called the police. The police recognized it as phreaking paraphernalia, including stolen Pacific Bell manuals and fake IDs. The police linked Poulsen to the storage unit and called him in for questioning; he denied doing anything illegal. When FBI agents searched Poulsen's home, they found evidence linking him to hacking but thought something more sinister was afoot. The FBI suspected Poulsen was hacking classified systems and violating national security. More precisely, they thought he had been selling U.S. secrets to other countries.[74]

In November 1989 a grand jury indicted Poulsen and two co-defendants on 18 counts of computer and telecommunications fraud. The others surrendered, but Poulsen fled before FBI agents could arrest him and then called the FBI to taunt them for letting him escape.

While hiding in Los Angeles, Poulsen used his phreaker and hacker talents in a money-making scheme. A radio station was giving away $50,000 Porsches, one a week to the 102nd person to call after a DJ played

three songs in sequence.[75] Poulsen hacked the phone company's computers and diverted the radio station's incoming calls to a line he controlled. When a DJ played the songs, Poulsen counted calls that had come in, intervening when it reached 60. Then he took over the station's phone line and counted down as the number approached 102. When it was close, Poulsen and a confederate known as "Agent Steal" began calling to ensure theirs was the 102nd call. They used this system to win two Porsches from the first radio station; they also used it to win $20,000 in cash from another radio station and two trips to Hawaii plus $2,000 in cash from a third radio station.[76] Poulsen sold one Porsche and used the money for living expenses.

Frustrated by their inability to catch him, the FBI arranged for the television show *Unsolved Mysteries* to air a segment on Dark Dante.[77] When Poulsen heard about the show, he sent the program a letter, saying it would slander him.[78] A few hours before the show aired, an *Unsolved Mysteries* secretary took a call she found odd: Instead of leaving a tip, the caller wanted the toll-free number people called to provide tips. She found that odd because the number was displayed on the screen when the program was on the air.[79]

The Dark Dante segment was scheduled for October 10, 1990. When *Unsolved Mysteries* aired that evening, its phones went dead before the show got to its segment on Poulsen. No one could reach *Unsolved Mysteries* to submit tips about Dark Dante. Many think Poulsen shut down the phone lines; such a feat would presumably not have been beyond such a talented hacker and phone phreak.[80]

Poulsen was finally captured six months later, on April 11, 1991. He was caught after the FBI got a tip he had been at a grocery store in Van Nuys. When agents showed his photo to store employees, they identified Poulsen as a man who had been there but had not come in for several weeks. An agent staked out the store after the FBI heard he had been back. On April 11, Poulsen came to the store and was arrested.[81]

On June 14, 1994, Poulsen pled guilty to computer fraud, mail fraud, money laundering, wiretapping, and obstructing justice. On February 9, 1995, Poulsen was sentenced to serve 51 months in prison and pay almost $58,000 in restitution for the radio station scams.[82] It was, at the time, the "longest prison sentence ever received by a hacker."[83] Poulsen was released from prison on June 4, 1996, because he was given credit for time he served while awaiting trial and sentencing. In all, he spent more than five years in prison, the "longest any computer hacker" had served to that point.[84]

One journalist called Poulsen "the last hacker," because Poulsen's career began when hacking was still seen as a playful intellectual exercise and ended when it was morphing into something much darker: cybercrime.[85] The term